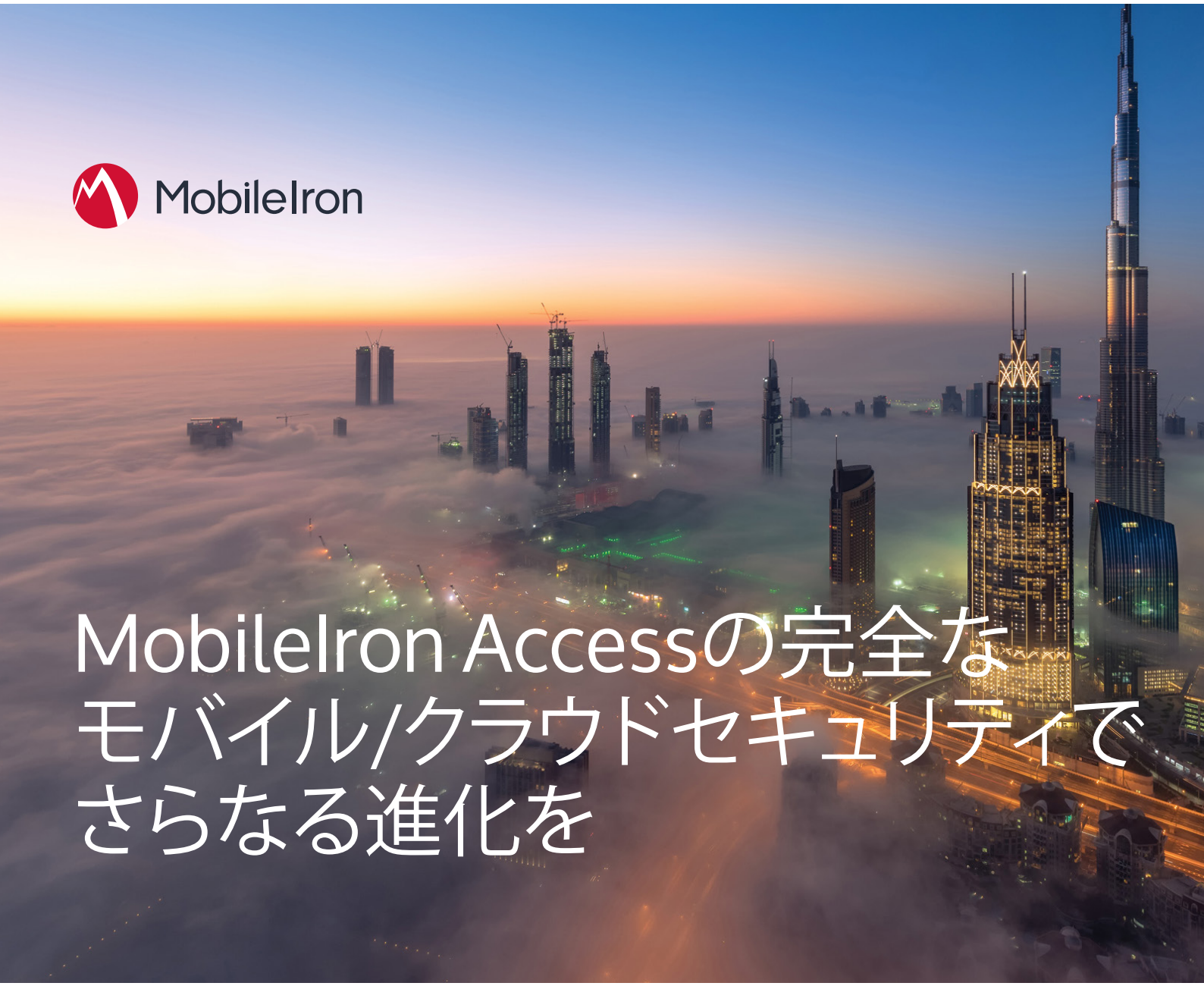


MobileIron Accessの完全なモバイル/クラウドセキュリティでさらなる進化を

MobileIron Access：完全なクラウドベースのセキュリティ

包括的なセキュリティ
MobileIron Accessは、デバイスおよびアプリの状態、ユーザーID、位置情報などを活用し、信頼できるデバイス、アプリ、ユーザーのみに企業向けクラウドサービスへのアクセスを提供します。

統合プラットフォーム
MobileIron Accessは、導入の容易な統合プラットフォームとして、モバイル/クラウド環境でビジネスアプリやデータのセキュリティを確保します。

標準規格ベースのセキュリティ
MobileIron Accessは、大手のIDプロバイダーと簡単に統合でき、SAML 2.0規格に対応するあらゆるクラウドサービスのセキュリティを確保します。カスタム統合は必要ありません。

モバイル/クラウドセキュリティの課題

世界中の企業組織が、これまでにないペースで、クラウドベースのサービスやモバイルエンドポイント技術の採用を進めています。現代的なモバイル/クラウド技術への移行により、企業はエンドポイントセキュリティ対策の根本的な見直しを余儀なくされています。デスクトップベースの従来型のセキュリティモデルでは不十分だからです。

IT部門が管理するデスクトップPCの時代なら、ユーザー名とパスワードだけで情報アクセスのセキュリティを確保できました。モバイル/クラウド環境には、IDのみのセキュリティでは不十分です。デバイスやアプリの状態を検証するメカニズムがなく、安全でない行動が助長されたり、ユーザー体験が複雑化したりするためです。たとえば、IDのみのセキュリティでは、ユーザーが脱獄したモバイルデバイスを使ってビジネスアプリにアクセスしているかどうかを判断できないため、ビジネスデータが危険にさらされる恐れがあります。また、ユーザーが簡単に覚えられる脆弱なパスワードを作成したり、個人用のGoogleドキュメントなど、簡単にアクセスできるセキュアでない場所にパスワードを保存したりする場合もあります。さらに、モバイルの小さな画面で複雑なパスワードを入力するのは、モバイルデバイス上でビジネス文書やデータにアクセスしようとする企業ユーザーにとって大きなフラストレーションとなり得ます。誤った認証情報を複数回入力すれば、アカウントがロックされる場合もあります。

本書では、現在のモバイル/クラウド企業が対処する必要のある重大なセキュリティの問題点を取り上げます。

- **セキュアでないデバイス。**セキュアでないデバイスでは、ユーザーがデバイス上のアプリやブラウザに自身の認証情報を入力するだけで、モバイルアプリやクラウドサービスから簡単にビジネスデータにアクセスできます。デバイス上では、データが不正な外部ソースによって簡単に侵害されたり、共有されたりする可能性があります。セキュアでないデバイスには、iOS、AndroidまたはWindows 10などの最新OSを実行していても、モバイルデバイス管理（MDM）プラットフォームに登録されていないデバイスも含まれます。ドメインに参加していないWindows 7マシンもセキュリティ侵害に対して脆弱である場合があります。
- **非マネージドアプリ。**一般的には、Office 365生産性向上アプリなど、ユーザーが企業向けアプリストアではなく個人用アプリストアからダウンロードしたビジネスアプリが含まれます。結果としてこれらのアプリは、IT部門の管理下にない状態のまま、ユーザーが各自の認証情報を入力すればビジネスコンテンツへのアクセスに利用することができます。IT部門は非マネージドモバイルアプリに対する可視性を持たず、管理もしていないため、その後、データが他のデバイスやアプリと共有される可能性があります。
- **無許可のクラウドサービス。**ほとんどの企業向けクラウドサービスは、APIを使用して統合されるアプリやサービスのエコシステムと関連付けられています。企業向けクラウドサービスが許可されたものであっても、そのエコシステムからのアプリやサービスが許可されたものでない場合があります。つまり、ユーザーが自身の認証情報を利用して、無許可のサードパーティのサービスを企業向けクラウドサービスに接続できる可能性もあります。この場合、IT部門が知らないうち、あるいは制御できない状態で、無許可のクラウドサービス経由でビジネスデータがアクセスされたり、共有されたりします。

モバイル/クラウドセキュリティのベストプラクティス

モバイル/クラウドインフラにおけるセキュリティの穴を最小化するには、実証されたベストプラクティスにより、性能や生産性を損なうことなく、IT部門に管理と可視化の機能を提供する必要があります。企業には、プラットフォーム内でこれらのベストプラクティスとシームレスに統合する包括的なモバイル/クラウドセキュリティソリューションが必要です。

あらゆるクラウドサービスやモバイルOSでコンテキストポリシーを適用

企業ユーザーは、社内のアプリやクラウドサービスへのアクセスにおいてモバイルデバイスへの依存度を高めています。セキュアでないデバイス、非マネージドアプリ、無許可のクラウドサービスからのアクセスをIT部門が遮断するには、IDを利用したセキュリティだけでは足りません。モバイル/クラウドセキュリティには、IT部門がデバイスのタイプや状態、モバイルアプリの状態、クラウドサービスのタイプおよびユーザーIDに基づいて条件付きアクセス制御ポリシーを定義し、適用するのに役立つ最新のマルチOSプラットフォームが必要です。

シームレスなSSOでユーザー認証を簡素化

従業員の生産性向上は、組織がビジネスプロセスをクラウドへ移行する大きな理由の1つです。クラウドサービスにアクセスするたびにパスワードの入力を要求するのは、従業員と業務に必要なリソースの間に障害を作るようなものです。ユーザーは、パスワードを忘れるだけでなく、モバイルの小さな画面で認証情報を何度も誤入力し、ロックがかかってヘルプデスクに助けを求めることも少なくありません。このような状況は、従業員の生産性を停滞させ、サポートコストの増加や効率の低下にもつながります。結果的に、組織はシングルサインオン（SSO）などの技術を利用して、セキュアなアクセスを簡素化する必要があります。

コンプライアンスレポートの追跡と管理

セキュアなクラウドサービス、アプリ、デバイスを展開するだけでなく、IT部門には、セキュリティポリシーを適用し、コンプライアンスの追跡、監視、レポート作成を行うための、拡張性に優れた一元管理の方法が必要です。従来型ソリューションでは、従業員が企業向けクラウドサービスへの接続に使用するデバイスまたはアプリの状態に対して信頼性の高い可視性を提供できません。さらに、通常はIT部門が個々のクラウドサービスからログを収集し、それらを別のソースから得たログに手動で関連付けて、コンプライアンスに違反するデバイスやアプリを識別しなければなりません。このアプローチは非常に断片化されており、本当の意味での拡張性に欠けます。一般データ保護規則（GDPR）などの政策によってコンプライアンスガイドラインが厳しくなるにつれ、組織には、レポート作成、監査、是正を簡単に実行できる総合的なレポート作成プラットフォームが必要となります。

従来のアプローチの欠点

現在市場には、モバイル/クラウドセキュリティにおける個々の問題を解消するためのさまざまなソリューションが出回っていますが、それらは、前述の包括的なベストプラクティスには対応していません。

- **ID/アクセス管理（IAM）**
  IAMでは主に、ID/アクセス管理とアクセス制御に重点が置かれます。IAMソリューションは、クラウドサービス向けのIDベースのアクセス制御を提供しますが、デバイスまたはアプリの状態に基づいてアクセスを許可または拒否する機能はありません。

- **モバイルデバイス管理（MDM）**
  MDMでは、モバイルデバイスのセキュリティ保護に重点が置かれます。すべてのMDMベンダーがクラウドセキュリティに十分に対応しているとは言えず、多くのベンダーは、前述の非マネージドアプリや無許可のクラウドの問題を解決することができません。
- **クラウドアクセスセキュリティブローカー（CASB）**
  CASBは、クラウドサービス向けに、可視化機能と詳細なファイルレベルのアクセス制御およびデータセキュリティを提供します。しかし、デバイスのプロファイリングやデバイスの状態の判断、およびコンプライアンス違反のデバイスまたは無許可のアプリが企業向けクラウドサービスにアクセスすることを防止するといった点では、非常に限られた機能しかありません。

これらのソリューションは一般的に、それぞれの個別の機能を実行するものであり、統合が難しいサイロ化されたソリューションであるため、セキュリティの穴が生じ、ビジネスデータに脆弱性が残ります。

MobileIron Accessが統合されたモバイル/クラウドセキュリティを提供

Box、G Suite、Office 365、Salesforceなどの企業向けクラウドサービスを利用する企業には、これらのサービスのすべてに対応する条件付きアクセス制御が必要です。MobileIron Accessは、シームレスでセキュアなSSOと詳細な可視化機能により、セキュアなデバイス、マネージドアプリ、許可されたクラウドサービスのみにクラウド上の企業データを提供します。

他社の製品とは異なり、MobileIron Accessは、場所や使うデバイスを選ばず、ユーザーの生産性を確保しながら、クラウドサービスのセキュリティを保護する標準規格ベースの統合プラットフォームを提供します。このため、クラウドを出入りしてもビジネスデータのセキュリティが確保されます。

情報漏洩の防止

意図的な、あるいは意図しない従業員の行動による情報漏洩を防止することが非常に重要です。たとえば、ユーザーがSalesforceからファイルをダウンロードし、それらを個人のDropboxフォルダーにコピーするのを防ぐために、IT部門は何をすれば良いでしょうか？ 脱獄したiOSデバイス上で、CydiaストアのWebブラウザからSalesforceのデータへアクセスするのをブロックできるでしょうか？

MobileIron Accessは、条件付きアクセスポリシーによってこのような情報漏洩のリスクを軽減します。企業向けクラウドサービスとデータは、信頼できるユーザーが、コンプライアンス違反のないデバイスで、マネージドアプリと承認済みのクラウドサービスを使用した場合にしか提供されません。つまり、従業員がOffice 365などのマネージドクラウドサービスから取得したファイルやデータを、個人用のGoogleドライブなどの非マネージドアプリと共有することはできません。

ユーザー体験の強化

MobileIron Accessは、企業向けクラウドサービスに対応するシームレスでセキュアなSSOによってユーザー体験を改善します。ユーザーは、すべてのモバイルアプリやクラウドサービスにユーザー名とパスワードを入力しなくてもすぐにビジネスデータにアクセスできます。基本的なSSOと異なり、MobileIron Accessは、あらゆるモバイルアプリでシームレスに機能するため、セキュアでないアプリからのログインを防ぐことでセキュリティの層を追加します。

MobileIron AccessのSSOでは、認証情報の入力が最小限で済むため、認証情報の誤入力によるアカウントのロックが削減されます。ユーザーがヘルプデスクに問い合わせることなく自身で問題を解決できる直感的な修正ワークフローにより、生産性も向上します。

コンプライアンスレポート作成の簡素化

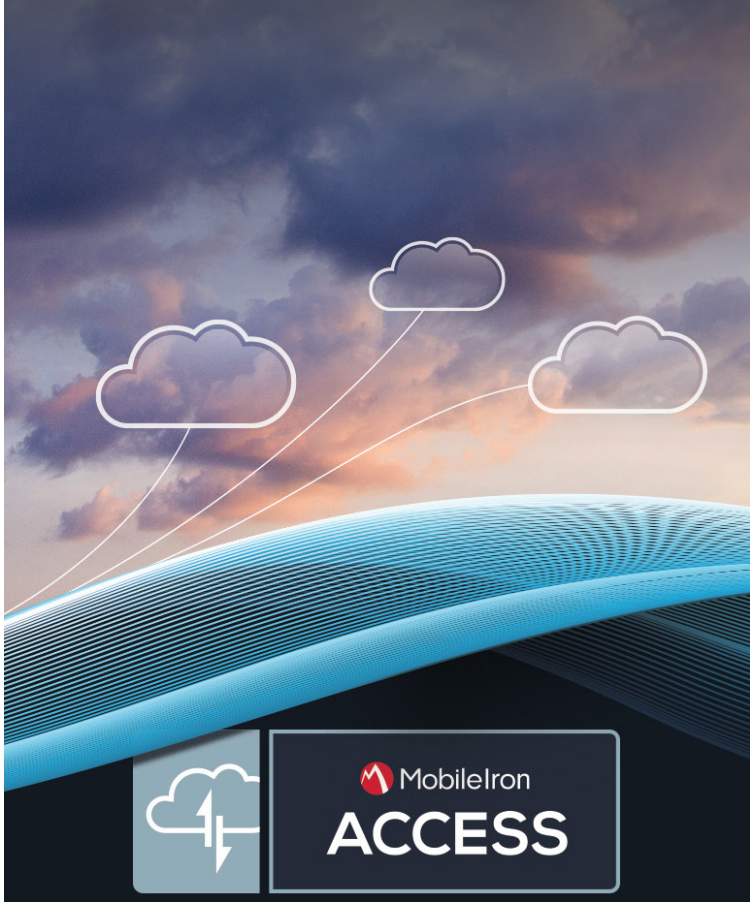
MobileIron Accessは、企業向けクラウドサービスに接続するすべてのデバイス、アプリ、サービス、位置情報、ユーザーを追跡する高度なレポート作成エンジンを装備し、詳細な可視化/監査機能によってコンプライアンスを推進します。このように詳細な可視化により、組織は、コンプライアンス違反のユーザーやデバイスをより簡単に特定し、コンプライアンス状態に戻すことができます。同様に重要なのは、MobileIron Accessでは、詳細なログ記録とレポート作成機能により、監査およびコンプライアンス監視が簡素化されていることです。

MobileIron Access：クラウドベースのビジネス改革のセキュリティ保護

モバイル/クラウド技術の普及は、世界中の組織に大きな変化を起こしています。これらの新技術により、組織は、ビジネスプロセスの合理化やコスト削減を実現し、従業員が場所を問わずに生産的に仕事を行えるよう支援することができます。しかし、モバイルアプリやクラウドサービスのセキュリティ保護には、モバイル/クラウド環境を想定していない従来型のPCベースのセキュリティアプローチでは不十分です。

現代企業には、MobileIron Accessのように、最初からモバイルアプリ、デバイス、クラウドサービスを想定して設計された包括的な統合プラットフォームが必要です。MobileIronでは、1つの制御点から、デスクトップPC、モバイルデバイス、最新のアプリおよびクラウドサービスを含む重要な企業のリソースのセキュリティを保護し、容易にビジネス改革を実現できます。

MobileIron Accessの詳細は、こちらをご覧ください：
mobileiron.com/access



MobileIron

〒106-0041
東京都港区麻布台1-11-10
日総第22ビル3階
www.mobileiron.com
Tel: +81.3.6426.5301
Fax: +81.3.6426.5302